Claims

What is claimed is:

1. A method of detecting unauthorized executable programs resident in a computer system memory comprising the steps of:

a) receiving a trusted hash value representative of a hash value for generation by a predetermined hashing process of predetermined data stored in memory within the computer system if an unauthorized executable program is other than resident in the computer system;

b) hashing the data stored in memory within the computer system using the predetermined hashing process to determine a computed hash value; and

c) comparing the computed hash value and the trusted hash value to determine differences between the data and the predetermined data.

2. A method of detecting unauthorized executable programs resident in a computer system memory according to claim 1 including the steps of

aa) receiving user authorization information;

aaa) authenticating the user authorization information to perform at least one of authorize and identify a user; and

aaaa) when the user is at least one of authorized or identified, requesting security data of the user.

3. A method of detecting unauthorized executable programs resident in a computer system according to claim 2 wherein the authorization data is at least a biometric information sample; and wherein the step of authenticating includes a step of comparing the at least a biometric information sample to a previously stored biometric template.

4. A method of detecting unauthorized executable programs resident in a computer system according to claim 2 comprising the steps of:

when the comparison is indicative of other than an unauthorized executable programs resident in a computer system, providing the requested security data relating to the user.

5. A method of detecting unauthorized executable programs resident in a computer system according to claim 1 comprising the steps of:

receiving a request for security data from an application in execution in the computer system; and,

when the comparison is indicative of other than an unauthorized executable programs resident in a computer system, providing security data to the application.

6. A method of detecting unauthorized executable programs resident in a computer system according to claim 1 wherein the trusted hash value and the computed hash value are determined by a same trusted security application executing locally on a processor of a same computer system at different times, the trusted hash value determined when the computer system is in a known secure state.

7. A method of detecting unauthorized executable programs resident in a computer system according to claim 6 wherein the trusted hash value is digitally signed.

8. A method of detecting unauthorized executable programs resident in a computer system according to claim 7 including the step of:

b1) verifying an authenticity of the digitally signed trusted hash value.

9. A method of detecting unauthorized executable programs resident in a computer system according to claim 8 comprising the steps of:

receiving a request for security data from an application in execution in the computer system; and,

when the authenticity of the digitally signed trusted hash value is verified and the comparison is indicative of other than an unauthorized executable programs resident in a computer system, providing the requested security data to the application.

10. A method of detecting unauthorized executable programs resident in a computer system according to claim 9 wherein the application and the predetermined hashing process are both executed on a same processor of the computer system.

11. A method of detecting unauthorized executable programs resident in a computer system according to claim 8 comprising the step of:

d) when the computed hash value and the trusted hash value are other than indicative of a known secure state, issuing a notification that an unauthorized executable program is detected within the computer system.

12. A method of detecting unauthorized executable programs resident in a computer system according to claim 11 comprising the step of:

e) when the computed hash value and the trusted hash value are other than indicative of a known secure state preventing access to the computer system.

13. A method of detecting unauthorized executable programs resident in a computer system according to claim 7 comprising the step of transmitting the trusted hash value to a second other computer system in communication with the computer system and retrievably storing the trusted hash value within the second other computer system.

14. A method of detecting unauthorized executable programs resident in a computer system according to claim 13 including the step of transmitting the computed hash value to the second other computer system for comparison with the trusted hash value by a processor of the second other computer system.

15. A method of detecting unauthorized executable programs resident in a computer system according to claim 14 wherein the computed hash value is a value determined in dependence upon the predetermined data existing in memory within the computer system and some time dependent data of the computer system.

16. A method of detecting unauthorized executable programs resident in a computer system according to claim 14 wherein the second other computer system includes a trusted source wherein security data is stored for provision to applications in execution on systems that are known to be secure.

17. A method of detecting unauthorized executable programs resident in a computer system comprising the steps of:

a) providing a trusted security application executable on a processor of the computer system for determining a hash value using a predetermined hashing process of predetermined data existing in memory within the computer system;

b) hashing the data existing in memory within the computer system using the predetermined process to determine a hash value;

c) digitally signing the hash value to provide a trusted hash value; and

d) retrievably storing the trusted hash value,

wherein the hash value is determined absent an unauthorized executable program being present within the computer system; and

wherein the predetermined data relates to programs in execution on the processor of the computer system.

18. A method of detecting unauthorized executable programs resident in a computer system according to claim 17 comprising the steps of:

e) comparing a computed hash value with the trusted hash value to detect changes to the predetermined data existing in memory within the computer system.

19. A method of detecting unauthorized executable programs resident in a computer system according to claim 18 comprising the step f) verifying the authenticity of the digital signature of the trusted hash value.

20. A method of detecting unauthorized executable programs resident in a computer system according to claim 19 comprising the step of:

g) when the computed hash value and the trusted hash value are indicative of a same trusted state of a computer system, providing security data from a trusted source to an application in execution on the system.

21. A method of detecting unauthorized executable programs resident in a computer system according to claim 20 comprising the step of:

h) when the computed hash value and the trusted hash value are other than indicative of a same secure state of the system, notifying a system administrator.

22. A method of detecting unauthorized executable programs resident in a computer system according to claim 1 wherein predetermined data includes DLL tables.

23. A method of detecting unauthorized executable programs resident in a computer system according to claim 1 wherein predetermined data includes system memory locations indicative of executable programs in operation.

24. A method of detecting unauthorized executable programs resident in a computer system according to claim 1 wherein predetermined data is hashed in an absolute memory location independent fashion.